Statewide Information Security Manual Review and Updates

2012-2013 Review Period

Enterprise Security and
Risk Management Office

Goal	Section	Title	Comments/Update	Work Comments
Review/Revise terminology of "statewide information security standards" throughout manual	All	All	To be consistent make sure that the terminology is either "statewide information security standards" or "statewide security."	Modified statements throughout manual to be "statewide information security standard(s)."
Correct Table of Contents	Table of Contents	Table of Contents	Missing chapter 8 p. 156 entry. Chapter 8 - Developing and Maintaining In-House Software.	Corrected table of contents.
Define "Significant change"	Introduction	Introduction	Reword sentence with "significant change" to better convey meaning.	Added PCI DSS in list of standards and statutes to which agencies may need to supplement the policy manual. **Response to customer**. Significant change is defined by the agency.
Include additional industry standards for compliance	010101	Defining Information	Include statement about complying with all applicable standards (i.e. PCI DSS) and not just federal and state statutes.	Modified standard to state the following: "Complying with applicable federal and state laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and all applicable industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS)."
Modify criticality and value to confidentiality	010102	Labeling Classified Information	Most documents are labeled to address their confidentiality, not criticality and value. Consider revision.	No change. **Response to customer.** While data is generally classified by it's confidentiality, non-confidential data could still be critical to an organization's operations and should therefore be classified as such.
Review/revise data sharing standards/guidelines	010103	Storing and Handling Classified Information	Make it clear that the sharing of data needs to be agreed to the highest level and the agency receiving the data becomes co-owner of the data and is just as responsible. Consolidate standard.	Moved and reworded the following statement from 030710 – Transporting Confidential Documents: "Agencies shall ensure that confidential information is properly protected in transport or transmission." Moved and reworded the following standard from standard 030521 – Using Customer and Other Third-Party Data Files: "Agencies shall ensure that all confidential information and related files under the agency’s control in electronic format are handled properly and secured accordingly. Use of such information shall be in compliance with all applicable laws, and regulations, and limitation imposed by contract(s)."
Consolidate standard	010103	Storing and Handling Classified Information	Consolidate standard.	Moved the following guidelines from 030701 - Managing Hard-Copy Printouts: "Documents that contain confidential information should be restricted to authorized personnel. Any person who prints or photocopies confidential data should label and control the original and copied document in accordance with all applicable policies, statutes and regulation. Proper retention, archive and disposal procedures for such documents should be observed."
Revise encryption statements	010103	Storing and Handling Classified Information	Minimum encryption strength is not clearly provided in manual for data at rest. Also, footnote #3 refers to a chapter not in manual.	Removed footnote to reference to Statewide Technical Architecture. Added the following statement: "See standard 030203 - Controlling Data Distribution and Transmission for the minimum requirement for encrypting data in transit." **Response to customer**. Minimum encryption strength for data at rest is defined in standard 030801.
Consolidate standard	010105	Classifying Information	Consolidate standard.	Moved the following statement from 010106 - Accepting Ownership for Classified Information: "Agency custodians of data and their designees are responsible for agency data and shall establish procedures for appropriate data handling." Moved the following guideline from 030519 - Using Headers and Footers: "State employees should consider using document headers and footers to notify readers of files classified as confidential."
Consolidate standard	010106	Accepting Ownership for Classified Information	Consolidate standard.	Moved standard to 010105 – Classifying Information.
Consolidate standard	010107	Managing Network Security	Consolidate standard.	Moved standard to 030102 - Managing the Networks.
Define/clarify "Standard user profiles" and "Restriction of connection time"	020101	Managing Access Control Standards	Reword bullet with "Standard user profiles" to better convey meaning. Clarify meaning for "Restriction of connection time". Clarify if "predetermined times for processing those data must be set by the interested parties to protect the integrity of the data" is for all data or just high risk data. Add PCI DSS requirements.	Added the following PCI DSS requirements: "Assignment of privileges shall be based on an individual’s job classification, job function, and the person’s authority to access information. Default access for systems containing confidential information shall be deny-all." Reworded bullet for user profiles to say "User profiles that define roles and access." Reworded bullet for termination of access to say "Termination of employment." Added the following statement: "Agencies shall modify an individual’s access to a State information technology asset upon any change of employment or change in authorization, such as a leave of absence or temporary reassignment." Clarified last paragraph to include "all data."

Goal	Section	Title	Comments/Update	Work Comments
Review UserID/Password terminology. Consider "credentials".	020102	Managing User Access	Review instances of userID and Passwords. May we use "credentials" to include both userIDs/Passwords and other forms of credentials such as tokens?	Replaced instances of "User ID" with "User credentials." Added the following statement: "user's credentials, such as user IDs, ID cards, tokens, and biometrics." Added the following PCI DSS requirements: "There shall be a documented approval process whereby authorized parties specify required privileges for user access. Agencies shall communicate user account policies and procedures including authentication procedures and requirements to all users of an information system." AND "Default/generic user accounts and passwords shall be disabled or changed prior to a system being deployed in production." Added statements regarding sharing credentials: "User credentials shall not be shared but only used by the individual assigned to the account." Renamed section on "Outside User IDs" to be "Non-employee Credentials."
Update standard on user's locking workstations	020103	Securing Unattended Work Stations	Consolidate standards on locking workstations	Moved standard 050706 to 020103. Standard 020103 now includes the following statement: "Users shall lock their workstations when leaving them unattended. When not in use for an extended period of time, as defined by the agency, each desktop/laptop shall be logged off. Removed requirement for users to shall turn off computers at the end of the day."
Revise reference to "State CIO's Use of State Network and the Internet Standard"	020104	Managing Network Access Controls	"State CIO's Use of the State Network and the Internet Standard" is not referenced elsewhere in the manual and no link it provided for obtaining this document.	Removed reference to old policy and modified standard to say the following: "When users on the agency networks connect to external systems, including the State Network, they shall comply with all state and agency acceptable use policies."
Review/revise use of "modem"	020104 020112	Managing Network Access Controls	Consider changing "modem" to reflect all technologies that could potentially create a multi-homed environment. (e.g. users shall not be multi-homed while using the State Network). Please consider Fax's and MFP when looking at this standard.	In 020104, replaced "modem" with "telecommunications device." Also replaced "modem" with "telecommunications device" in 020112 where applicable.
Review/revise wording for programs altering systems	020105	Controlling Access to Operating System Software	Some programs can alter systems without using operating system commands. It could more appropriately read "alter the operating system (e.g. run operating system commands, install programs, remove programs, change configuration)"	Changed phrase in the first paragraph to be "operating system administrative commands and programs."
Review standard	020106	Managing Passwords	This leaves out other types of credentials such as tokens and PINs. This standard could be extended to all types of credentials.	Changed instances of "user ID" to be "user credential." Reworded second paragraph to begin with "An information system's." Changed minimum number of characters for a password to be 8 characters. Removed the bullet for 6 character passwords and made the following statement: "Where technically feasible, passwords shall be at least eight (8) characters long for access to all systems and applications." Moved the following statement from 100302 – Keeping Password/PIN Numbers Confidential: "Attempts to gain access to a user's password through these social engineering means (i.e. phishing) must be reported to the agency security administrator." Added the following PCI DSS requirement: "There shall be a process for validating the identity of an end user who requests a password reset. Initial passwords and subsequent password resets shall utilize a unique password for each user account."
Review standard	020106	Managing Passwords	How long must information be maintained? Is this left to the agency to determine the reasonableness of time to maintain this information?	Modified the following statement to address records retention for logon attempts: "In order to facilitate intrusion detection, information shall be retained on all logon attempts in accordance with agency records retention policy or the General Schedule for State Agency Records, Information Technology Records."
Review standard	020106	Managing Passwords	This standard requires that the State CIO approve of all single sign-on solutions and maintaining of password list. How is this approval granted for systems such as Active Directory? Does this standard need to be broadened to include appropriate agency approvals?	**Response to customer.** No. The State CIO must approve the use of single sign-on solutions. Active Directory is not currently considered a single sign-on solution.

Goal	Section	Title	Comments/Update	Work Comments
Review standard	020106	Managing Passwords	Since this standard doesn’t specify the type of encryption required this could include basic encryption such as word level encryption which is easily reversible. This could be revised such that the security administrator for the agency would have to approve the level of encryption for sending electronic communication based off risks.	Modified statement on password encrption to say the following: "Where possible, applications that require clear-text authentication shall be converted to equivalents that can use agency approved encryption."
Clarify audit trail requirement	020107	Securing Against Unauthorized Physical Access	Clarify physical access requirements to data center housing information technology assets or regular information assets such as workstations. Suggest that this be mandatory for data centers but based on risk for other types of physical facilities.	Moved standard to 090104 - Physical Access Control to Secure Areas.
Revise standard	020108	Restricting Access	Clarify statements regarding third party access.	Removed paragraph regarding third party access. Access control requirements are mentioned elsewhere in manual.
Clarify situation of user change	020112	Controlling Remote User Access	Please clarify the scenario described in standard regarding changing a active user ID. Is this a reference to remote access, access to an administrator (e.g. root) account locally. Please clarify this in the manual in order to clearly outline what protections should be in place for changing account access levels. What does this mitigate?	Modified statement to include an example: "If users employ system facilities that allow them to change the active user ID to gain certain privileges, such as the switch user (su) command in Unix/Linux, they must have initially logged in employing a user ID that clearly indicates their identity."
Combine standards 020112 and 030103	020112	Controlling Remote User Access	Combine standard with 030103 - Accessing Your Network Remotely.	Moved most of 030103 - Accessing Your Network Remotely into 020112. Replaced "user ID" with "user credential" where applicable.
Review session timeout requirement	020112 030109	Controlling Remote User Access	Review/update session timeout requirement.	Added the following: "For some higher risk information systems, the requirement for a session idle timeout may be more stringent as determined by agency policy, industry standards (i.e. PCI DSS) or other regulations."
Consolidate standard	020113	Types of Access Granted to Third Parties	Consolidate standard.	Moved standard to 020108 - Restricting Access.
Consolidate standard	020114	Why Access is Granted to Third Parties	Consolidate standard	Moved standard to 020108 – Restricting Access.
Review/update Access Control Framework	020115	Access Control Framework for Network Security	Consider adding requirements/zone for storage area networks (SAN).	**Response to customer.** A Storage Area Network (SAN) is a type of technology. The Access Control Framework defines requirements for data, not technology.
Review/update Access Control Framework	020115	Access Control Framework for Network Security	Review/update Access Control Framework requirements. Include changes for IPS requirements and State WAN designation. Consider making IPS/IDS required for management domain.	Modified standard throughout to use the word "matrix" instead of "template" to make it more consistent. Made IDS/IPS Host optional throughout the matrix. Merged State WAN columns (Std/High) into one column. Modified footnote to Matrix concerning firewall requirements to state the following: "Refer to 030107 Routing Controls and Firewall Configuration standard." Added the following statement in the footer of the Access Control Framework Matrix regarding IDS/IPS: "Minimum security level for IDS/IPS deployment in the enterprise infrastructure is determined by the SCIO."
Review Access Control Framework requirements for HVAC	020115	Access Control Framework for Network Security	More detailed guidance should be given to determine "appropriate access control mechanism". Clarify logical separation.	Modified statement regarding requirement for exclusion of facility management systems to say the following: "...those systems are not publicly accessible, are logically isolated (i.e. VLANs) from other networked systems and cannot access other shared systems/services, and have appropriate access control mechanisms in place, such as Access Control Lists (ACLs), authentication mechanisms, or a VPN."
Clarify "cloud computing" requirement	020115	Access Control Framework for Network Security	The standard only requires that cloud computing services have to adhere to the Statewide Security Standard. This leaves out other services that are provided to the state that fall outside the definition of cloud computing. We recommend including language that would be inclusive of all services, rather than just those deamed to be "cloud computing")	Modified statement on cloud computing to say the following: "Vendors of cloud computing services or other types of hosted solutions shall agree to comply with all statewide information security standards when the State utilizes such services through SLAs and contracts."

Goal	Section	Title	Comments/Update	Work Comments
Define/clarify "where feasible" and "physically separated"	020115	Access Control Framework for Network Security	What is the definition of physically separated? Does this mean that virtual disk shall be separated on different stores or does this mean separate virtual machine servers should be running high risk applications.	Modified statement regarding physically separate virtual machine based upon risk to say the following: "Agencies should consider separating high risk virtual machine farms from lower risk virtual machine farms on to separate physical servers."
Clarify two-tier applications and direct user access to database	020115	Access Control Framework for Network Security	Please clarify whether this standard allows for two tier architecture where clients touch the application server and that contacts the databases. Also, define where if any a client-server model is allowed in the Framework, i.e. end user direct connection to a database through an application. Include examples of Access and FoxPro as client-server DBs.	Added the following statements regarding two-tier applications and direct user access to a database: "Where end user access is allowed to a resource, it is designated with “Opt.” for optional. Client-server applications that operate on an agency local area network (LAN) and are not public facing (i.e. Internet accessible) may fall under the Agency Internal LAN column of the matrix below."
Clarify special assembly zones	020115	Access Control Framework for Network Security	Clarify process for creating a special assembly zone.	Added the following statement: "Agency CIOs shall develop a process for creating Application Unique Domain (AUD) special assembly zones and maintain a list of their AUDs. Agencies must also report to the State CIO their AUD special assembly zones."
Clarify auditing requirements for the Access Control Framework	020115	Access Control Framework for Network Security	Statewide Security Standard 020110 requires that all access be audited every 6 months and every 3 months for privileged accounts. Please clarify if all data access must be audited every six months or does certain types of data only need to be audited on an ad-hoc basis per 020115.	Changed zone audit requirements for user accounts to be "Required" throughout the zones. Removed row for "Data Access Audit."
Review/update Access Control Framework	020115	Access Control Framework for Network Security	The encrypted channel does not define the minimum algorithm and strength for confidential data or system administrator access. What are the minimum requirements for the encryption channel (e.g. TLS version 1.2 and above or AES-256 for confidential information).	**Response to customer**. See 030203 - Controlling Data Distribution and Transmission for minimum requirement for encrypting data in transit.
Remove duplicate standard	020116	Managing User Access	Remove duplicate standard	Removed standard. 020102 - Managing User Access states these requirements.
Review references to "business" and "State"	020117	Controlled Pathway	Please change references from business to State to line up with the Standard verbiage.	Changed "business" to "state" in standard.
Review standard	020119	Diagnostic and Configuration Port Controls	Removed standard and guidelines.	Removed standard because it is mentioned in 020112 - Controlling Remote User Access. Removed guideline because it is a standard in 020105 - Controlling Access to Operating System Software and 030308 - Setting Up Internet Access.
Add PCI DSS requirements	020121	Acceptable Usage of Information Assets	Add PCI DSS requirements.	Added the following PCI DSS requirement: "AUPs shall define the proper use of information assets and shall include critical technologies such as remote access technologies, removable electronic media, laptops, tablets, smartphones, e-mail usage and Internet usage." Removed guidelines.
Review standard	020123	Third Party Service Management	Move 020124 - 020124 Monitoring Third Party Services into this standard.	Moved 020124 – Monitoring Third Party Services into this standard. Standard now states the following: "Services, outputs and products provided by third parties shall be reviewed and checked regularly. To monitor third party deliverables, Agencies shall: o Monitor service performance of third party vendor to ensure service levels are up to contract requirements. o Review reports provided by third parties and arrange regular meetings as required by contract(s). o Provide information concerning security incidents to the Enterprise Security and Risk Management Office (ESRMO). o Review third party reports including the following, but not limited to, audit logs, operational problems, failures, fault analysis, as they relate to services being delivered, including security events. o Resolve and manage any identified problem areas."
Review standard	020124	Monitoring Third Party Services	Moved standard into 020123	Removed standard and moved content into 020123 - Third Party Service Management.

Goal	Section	Title	Comments/Update	Work Comments
Consolidate standard	030102	Managing the Networks	Consolidate standard about managing network security.	Moved the following statement from standard 010107 - Managing Network Security: "Agencies shall manage the network security of their respective agencies based on business needs and the associated risks." Moved the following statements from 010107 - Managing Network Security and 030106 -Controlling Shared Networks: "Access to information available through the State network shall be strictly controlled in accordance with approved access control policies and procedures. Users shall have direct access only to those services that they have been authorized to use."
Remove standard 030103	030103	Accessing Your Network Remotely	Combine standard with 020112 - Controlling Remote User Access.	Removed standard and moved most of content to 020112 – Controlling Remote User Access.
Consolidate standard	030104	Defending Network Information from Malicious Attack	Consolidate standards on monitoring and reviewing system usage.	Moved the following statements from standards 130408 - Risks in System Usage and 130409 - Reviewing System Usage into this standard: "Monitoring and reviewing system usage for activities that may lead to business risks by personnel who are able to quantify and qualify potential threats and business risks. Appropriate controls and separation of duties shall be employed to provide review and monitoring of system usage of personnel normally assigned to this task. • Over utilization of bandwidth. • Un-authorized login attempts. • Un-authorized attempts to make changes to system settings. • Trending activity, such as to monitor for repeated information security attacks."
Consolidate standard	030106	Controlling Shared Networks	Consolidate standard.	Moved some of standard into 030102 - Managing the Networks.
Review firewall requirements	030107	Routing Controls, including Firewall Configuration	1) Do these firewall requirements apply to host-based and other software firewalls as well as network firewalls? 2) Do these requirements apply to all devices that implement network access control mechanisms (such as ACL's)?	Renamed title to be Routing Controls and Firewall Configuration. **Response to customer.** 1) Yes. 2) Yes.
Review firewall requirements	030107	Routing Controls, including Firewall Configuration	1) This standard now requires that agencies have at least 2 firewall administrators. One of those is required to be consulted before policy changes are approved and implemented. The term "administrator" is potentially confusing to some readers. 2) Is there an appropriate section elsewhere in this Security Manual that does/can/should address a similar requirement that a security specialist be consulted (or involved in the approval) of new system designs, system architectural changes, etc. that are not necessarily related to firewall changes. For example, if a new system or application is being implemented, should that design require the review, consultation and/or approval by a security analyst?	**Response to customer.** 1) The two firewall administrator must be two separate people, and at least one is consulted of a change and before it is implemented. The two firewall administrators do not need to approve changes, but at least one must be consulted before changes are implemented. One firewall administrator may consult the other person in the case of two administrators or another person authorized to make firewall changes at the agency. If the agency's Change Advisory Board (CAB) does not include the appropriate personnel as defined in this policy, the policy intent has not been met and a review meeting between one of the two firewall administrators and other(s), who either approve or implement the change, is required. The intent of this policy is to have a minimum of two firewall policy administrators, with at least one of them being a security specialist, to review firewall changes prior to implementation. One of the firewall policy administrators could be a manager of firewall configuration and device hardware. 2) No, no other section specifically states "security specialist" to be involved. The manual requires agency managment, security liaisons, and administrators to be involved in various aspects of operational security. Hardware designs are required to comply with state security policies.
Define minimum encryption strength	030107	Routing Controls, including Firewall Configuration	Does not define the minimum level of encryption required to store firewall passwords. No part of the information security manual addresses minimum security requirements for data at rest. Minimum encryption strength is not clearly provided in this manual.	**Response to customer.** Password encryption is not uniform across firewall vendors. Also, firewall devices shall be protected with physical security and console ports for administrative access.
	030108	Network Security	Clarify requirement for terms and conditions to upstream providers.	Removed statement regarding upstream providers. Standard now reads as follows: "ITS is responsible for the security of the infrastructure of the state's network."
Modify session timeout standard	030109	Time-out Facility	Clarify timeout standard in regards to higher risk systems	Added the following statement: "For some higher risk information systems, such as systems that process health care data, tax data, or credit card information, the requirement for a session idle timeout shall be 15 minutes or less, as determined by industry standards or other regulations."

Goal	Section	Title	Comments/Update	Work Comments
Clarify policy on storage of confidential data on personally owned devices	030203 & 030801	Controlling Data Distribution and Transmission	Add policy statement on protecting confidential data on personally owned devices.	Added the following statement to both 030203 and 030801: "Confidential data shall be encrypted when stored on non-State owned devices and only by authorized users. Federally protected confidential data shall not be stored on non-State owned/managed devices."
Add PCI DSS requirements	030205	Managing Electronic Keys	Add PCI DSS requirements.	Added "substitution" to the list of actions to protect electronic keys. Added the following bullets: "Cryptographic keys are replaced or retired when keys have reached the end of their life or the integrity of the key has been weakened or compromised", "Custodians of cryptographic keys formally acknowledge they understand and accept their key-custodian responsibilities." Added the following statement: "Agencies shall use strong cryptographic keys when protecting confidential data."
Add PCI DSS requirements	030206	Managing System Operations and System Administration	Add PCI DSS requirements. Move guideline concerning vendor-supported software.	Added the following PCI DSS requirements: "Develop and document daily operational security procedures." Moved guideline concerning vendor supported software into standard. Standard now reads: "Vendor-supplied software used in operating systems shall be maintained at a level supported by the vendor."
Clarify error logging requirements	030208	Monitoring Error Logs	This standard implies that error level logging must be enabled on all devices. What are the collection requirements for these logs. 1) Do the collected error logs have to be stored centrally? 2) Do confidentiality and integrity of these logs have to be protected?	Removed the following statement from the standard: "The confidentiality, integrity and availablity of error logs shall be safeguarded." **Response to customer.** 1) No. 2) No.
Clarify error logging requirements	030208	Monitoring Error Logs	The weekly monitoring requirement implies a significant level of burden on operations personnel. 1) Does every event need to be cross checked with known security events? 2) Does this standard apply if technologies such as SIEM are alerting on anomaly events (e.g. errors).	**Response to customer**. 1) No. 2) Standard applies but the SIEM is doing the weekly monitoring automatically.
Clarify error logging requirements	030208	Monitoring Error Logs	What is the record retention for error events and does that record retention depend on the applications that are storing, processing, or transmitting data over the network?	**Response to customer.** The administrative value only ends once the logs have been reviewed, which shall be at least weekly.
Consolidate standard	030211	Monitoring Operation Audit Logs	Consolidate standard. Add PCI DSS requirements.	Moved the following statements from 030219 - System Use Procedures into this standard: "Agencies shall implement a program for continuous monitoring and auditing of system use to detect unauthorized activity. All network components and computer systems used for agency operations must have the audit mechanism enabled and shall include logs to record specified audit events." Added the following PCI DSS requirements: "Audit logs of high risk information system, such as those that process credit card data, shall be reviewed on a daily basis." "Access to audit logs shall be restricted to only those authorized to view them and the logs shall be protected from unauthorized modifications, and if possible, through the use of file-integrity monitoring or change-detection software." "Audit files shall be written to a log server on the internal network and subsequently backed up to a secure location." "To the extent possible, audit logs shall include at least the following information when recording system events."

Goal	Section	Title	Comments/Update	Work Comments
Consolidate standard	030211	Monitoring Operation Audit Logs	Consolidate standard. Add PCI DSS requirements.	Added the following guidelines from 030219 - System Use Procedures and PCI DSS: "For audit logs on internal agency systems and network components, agencies should record, at a minimum, the following types of security-related events: o User login activity, both failed and successful, including user IDs, log-in date/time, log-out date/time. o Unauthorized access attempts to network or system resources, including audit files. o Changes to critical application system files. o Changes to system security parameters. o System start-ups and shut-downs. o Application start up, restart and/or shutdown. o Attempts to initialize, remove, enable or disable accounts or services. o Changes to the auditing function, including enabling or disabling auditing and changing events to be audited. o User credential creation and deletion. o Attempts to create, remove or set passwords or change system privileges. o All uses of special system privileges. o System errors and corrective action(s) taken. o Failed read-and-write operations on the system directory. o All actions taken with administrative privileges. Agencies should ensure that processing and storage capacity requirements are sufficient to capture and store the events cited above without adversely impacting operations. Agencies should also ensure that on-line audit logs are backed-up to protected media well before the on-line logs are filled to capacity so that no audit information is lost or overwritten."
Review standard	030212	Syncronizing System Clocks	Modify time syncronization standard. Add PCI DSS requirements.	Added "industry accepted" to the type of time source to be used. Added the following PCI DSS requirement: "Time synchronization data and configurations shall be protected from unauthorized modification."
Add PCI DSS requirements	030216	Third Party Service Delivery	Add PCI DSS requirements.	Added the following PCI DSS requirements: "Agencies shall develop a process for engaging service providers and maintain a list of all service providers who store or share confidential data." and "The SLA shall also state how the service provider is responsible for data stored or shared with the provider." Removed guidelines.
Consolidate standard	030219	System Use Procedures	Consolidate standard.	Removed standard and merged content with 030211 - Monitoring Operational Audit Logs.
Consolidate standard	030220	Internal Processing Controls	Consolidate standard.	Moved standard to 030221 – Corruption of Data.
Consolidate standard	030221	Corruption of Data	Consolidate standard.	Moved the following statement from standard 030220 - Internal Processing Controls: "Agencies shall develop clear policies, standards, and/or procedures to detect, correct, and manage corrupted data files." Moved the following statement from standard 030222: "o An example of a method to rebuild corrupted records or files from a last known good state is a transaction log or log of activities. Agencies should take precautions to ensure that the transaction or activity log does not contain the action that corrupted the data in the first place."
Consolidate standard	030222	Corrupt Data Controls	Consolidate standard.	Removed standard and moved content to 030221 - Corruption of Data.
Consolidate standard	030304	Receiving Electronic Mail	Consolidate standard.	Moved the following statement from 030708 - Receiving Unsolicited Mail: "Agencies shall protect State resources by not taking action on unsolicited commercial electronic mail."
Consolidate standard	030306	Setting Up Intranet / Extranet Access	Consolidate standard.	Moved content from standard 030307 - Setting Up Extranet Access into this standard. Revised standard to cover both Intranet and Extranet sites.
Consolidate standard	030307	Setting Up Extranet Access	Consolidate standard.	Removed standard and merged content with 030306 - Setting Up Intranet / Extranet Access.
Consider OWASP web standards	030309	Developing a Web Site	Recommend including web standards such as Open Web Application Security Project (OWASP)	Modified standard to state the following: "Industry standards for securing operating systems and Web server software, such as National Institute for Technology and Standards (NIST), the Open Web Application Security Project (OWASP), and SANS Institute guidelines, should be used for guidance in securely configuring and hardening Web sites." Moved the guideline regarding patch management into standard. The statement now says the following: "Agencies shall follow 040106, the Technical Vulnerability Management standard, for web server operating systems and its related applications in order to reduce the risk of known patch-related vulnerabilities."

Goal	Section	Title	Comments/Update	Work Comments
Clarify requirement to collect submitter's known IP address	030309	Developing a Web Site	1) How long must this data be stored? 2) It may be more accurate to state that one must collect the source address from which the communication is received. The submitter's actually IP address may be different (e.g. NAT'd or proxied connections). 3) Does this have to be reviewed and approved by legal for the privacy statements of these websites? Is there something from ITS stating that without a privacy statement that this information shall be collected by all state agencies?	Clarified standard in regards to collecting information. Standard now states the following: "Web sites that accept citizen or public input through a web form shall automatically collect the submitter’s known/received IP address along with a current timestamp, for example web server logs." Modified standard to address privacy statements: "Information collected shall be kept in accordance with state and agency retention policies and shall be mentioned in agency privacy statements." **Response to customer.** 1) In accordance with the state's and agency's retention policies. 2) Reworded standard. 3) Added statement to standard regarding privacy. Agencies shall include this information in their privacy statements. See also standard 120106 - Legal Safeguards against Computer Misuse.
Move guidelines regarding account used on servers to standard	030309	Developing a Web Site	Move guideline regarding web server accounts and password management to the standard.	Moved the following statement from the guidelines into the standard: "Any accounts used by a server, Web server, Web application, or any other related applications (considered service accounts) need to meet appropriate password management standards as established in 020106 - Managing Passwords."
Review standard	030311	Forwarding Email	Remove guideline.	Removed the following guideline: "Agencies should consider including these items in an agency’s individual acceptable use policy."
Review social networking standard and user credential standards	030312	Using the Internet for Work Purposes	Standard only requires that users pick different passwords (or credentials) for social networking sites. Recommend that this be expanded to include that all websites have a different ID and password not just the social networking sites.	Modified requirement to say the following: "To use a different user credential and password for each social networking and other non-State owned/hosted site. Accounts and passwords used to access social networking sites used by agencies shall never be the same as accounts and passwords used for other personal or professional business. In particular, an employee’s NCID username or password must never be used for access to any other site or account outside of State government."
Review standard	030316	Maintaining a Web Site	Remove guideline for reviewing and updating web site content	Renamed titie to be "Maintaining A Web Site." Removed the guidelines which stated the following: "Agencies should review and update the data contained within their Web sites on a six-month basis."
Review/correct footnote 21	030319	Instant Messaging Communications	URL in footnote is not correct.	Updated URL in footnote to https://www.scio.nc.gov/mission/itPoliciesStandards.aspx. Revised bullet in Guildelines regarding annual security awareness training to clarify statement.
Consolidate standard	030404	Receiving Misdirected Information by Facsimile	Consolidate standard.	Moved the following from 030408 - Receiving Unsolicited Facsimiles: "Agencies shall develop guidelines for handling the receipt of unsolicited facsimiles, including advertising material, as well as misdirected facsimiles."
Consolidate standard	030408	Receiving Unsolicited Facsimiles	Consolidate standard.	Removed standard and moved content into 030404 - Receiving Misdirected Information by Facsimile.
Define due diligence	030502	Managing Data Storage	Clarify "due diligence" of securing encryption keys. Clarify record retention rules. Add PCI DSS requirements.	Moved and modified the following from standard 030509 - Information Retention Standard: "Agencies shall protect the State’s information and comply with agency records retention policy or the General Schedule for State Agency Records, Information Technology Records." Regarding encryption keys, modified statement to say the following: "Agencies shall ensure encryption keys are properly stored (separate from data) and available, if needed, for later decryption." Added the following PCI DSS requirements as guidelines: "Agencies should keep stored public data to a minimum of what is necessary to adequately perform their business functions. Sensitive or confidential data that is not needed for normal business functions, such as the full contents of a credit card magnetic strip or a credit card PIN, should not be stored. Agencies should consider implementing a process (automatic or manual) to remove, at least quarterly, stored confidential data, like cardholder data, that exceeds the requirements defined in the agency’s data retention policy."
Consolidate standard	030506	Managing Folders / Directories	Consolidate standard.	Moved the following content from standard 030507 - Amending Direcrtory Structures into this standard: "Agencies shall establish and manage access controls governing the modification or amendment of the directory structures on network or shared drives."
Consolidate standard	030507	Amending Directory Structures	Consolidate standard.	Removed standard and moved content to standard 030506 - Managing Folders / Directories.
Review standard	030508	Archiving Documents	Remove standard.	Removed standard.
Consolidate standard	030509	Information Retention Standard	Consolidate standard.	Removed standard and moved content to standard 030502 - Managing Data Storage.

Goal	Section	Title	Comments/Update	Work Comments
Rename title	030510	Creating New Spreadsheets	Rename standard title	Renamed standard title to say the following: "Creating New Spreadsheets"
Rename title	030511	Creating New Databases	Rename standard title	Rename standard title to say the following: "Creating New Databases"
Review standard	030513	Updating Draft Reports	Remove standard.	Removed standard.
Review standard	030514	Deleting Draft Reports	Remove standard.	Removed standard.
Review standard	030515	Using Version Control Systems	Remove standard.	Removed standard.
Review requirements for audit records	030516	Sharing Data on Software and Information Systems	This requirement states that all information systems must maintain an audit record for individual actions on files and records. 1) Does this include all read access of all files? 2) Does this include all write access of all files? 3) Does this include the modification of any file? 4) How long must this audit record be maintained?	Clarified what actions shall be recorded. Added the following statement: "...such as when a file is modified. Audit logs shall be retained in accordance with agency records retention policy or the General Schedule for State Agency Records, Information Technology Records."
Consider adding NDA to requirement	030517	Updating Citizen and Business Information	Should include a section that encourages agencies to make custodians of state information have to sign an NDA as described in the 100110 since that section has been eliminated.	Revised sentence in standard to state the following: "Access to citizen and business or agency confidential data shall be controlled through various appropriate access control mechanisms." **Response to customer.** Manual includes standard 100104 - Using Non-Disclosure Agreements (Third Party). Agencies may include NDAs in their formal agreements with custodians.
Review standard	030518	Using Meaningful File Names	Remove standard.	Removed standard.
Consolidate standard	030519	Using Headers and Footers	Consolidate standard.	Removed standard and moved the following content from guidelines to 010105 - Classifying Information: "State employees should consider using document headers and footers to notify readers of files classified as confidential."
Consolidate standard	030521	Using Customer and Other Third-Party Data Files	Consolidate standard.	Removed standard and moved content to 010103 - Storing and Handling Classified Information.
Consolidate standard	030522	Saving Data/ Information by Individual Users	Consolidate standard.	Removed standard and moved the following content to the guidelines of 030602 - Backing Up Data on Portable Computers: "State employees should periodically save data files from their desktop and laptop computers to an appropriate backup drive or disk."
Consolidate standard	030602	Backing Up Data on Portable Computers	Consolidate standard.	Moved standard from 030522 - Saving Data/Information by Individual Users to a guideline here. The guildeline states the following: "State employees should periodically save data files from their desktop and laptop computers to an appropriate backup drive or disk."
Add PCI DSS requirements	030603	Managing Backup and Recovery Procedures	Add PCI DSS requirements.	Added the following PCI DSS requirements: "o Classify back up media so the sensitivity of the data can be determined. o Store media back-ups in a secure location, preferably an off-site facility. o Physically secure all back up media from theft and destruction. o Send media by secured courier or other delivery method that can be accurately tracked. o Ensure management approval for any media moved from a secure area. o Properly maintain inventory logs of all media and conduct media inventories at least annually."
Review standard	030604	Archiving Information	Remove standard.	Removed standard.
Consolidate standard	030701	Managing Hard-Copy Printouts	Consilidate standard.	Remove standard and merged guidelines to 010103 - Storing and Handling Classified Information.
Consolidate standard	030702	Photocopying Confidential Information	Consilidate standard.	Remove standard and merged guidelines to 010103 - Storing and Handling Classified Information.
Review standard	030703	Filing of Documents and Information	Remove standard.	Removed standard.
Review standard	030704	The Countersigning of Documents	Remove standard.	Removed standard.

Goal	Section	Title	Comments/Update	Work Comments
Review standard	030705	Checking Document Correctness	Remove standard.	Removed standard.
Review standard	030706	Approving Documents	Remove standard.	Removed standard.
Review standard	030707	Verifying Signatures	Remove standard.	Removed standard.
Review standard	030708	Receiving Unsolicited Mail	Remove standard.	Removed standard.
Review standard	030709	Style and Presentation of Reports	Remove standard.	Removed standard.
Consolidate standard	030710	Transporting Confidential Documents	Consolidate standard.	Moved content to standard 010103 - Storing and Handling Classified Information.
Review standard	030711	Shredding of Unwanted Hard Copy	Remove standard.	Removed standard.
Review standard	030712	Using Good Document Management Practices	Remove standard.	Removed standard. Guideline stated in 010103 - Storing and Handling Classified Information.
Add guideline for encrypting mobile communication devices. Correct table headers	030801	Using Encryption Techniques	Add guideline for agencies to consider encrypting all mobile communication devices. Correct table headers so they appear above the table on the same page.	Added the following guideline: "If possible, agencies should consider encrypting all mobile communication devices regardless of the confidentiality of the information stored." Added the following statement: "Confidential data shall be encrypted when stored on non-State owned devices and only by authorized users. Federally protected confidential data shall not be stored on non-State owned/managed devices." Corrected table.
Include tablet computers in encryptions requirements	030801	Using Encryption Techniques	1) Does this standard need to include tablets since they contain the same information as Netbooks but in a smaller form factor. 2) Why is the encryption strength for storage of confidential information on removable media weaker than notebooks, laptops, and netbooks? Recommend that the minimum level of strength be AES-256.	Copied the following from 030203 - Controlling Data Distribution to address encryption of data in transit: "Encryption algorithms for the transmission of confidential data include, at a minimum, Secure Socket Layer (SSL) RC4 128 bit algorithms, SSL Server-Gated Cryptography (SGC) 128 bit algorithms, TLS 1.11 128 bit algorithms, or those algorithms that are accepted and certified by the National Institute of Standards and Technology (NIST)." **Response to customer.** 1) Tablet devices are included. 2) AES-128 is sufficient for these devices and appropriate for current technology.
Review standard	030904	Using Photocopiers for Personal Use	Remove standard.	Removed standard.
Review standard	030905	Speaking to the Media	Remove standard.	Removed standard.
Review standard	030906	Speaking to Customers	Remove standard.	Removed standard.
Review standard	030907	Need for Dual Control/ Segregation of Duties	Remove standard.	Removed standard.
Review standard	030912	Checking Customer Credit Limits	Remove standard.	Removed standard.
Review standard	040102	Selecting Business Software Packages	Modify standard for out-of-support software.	Moved guideline for avoiding software with no support into standard. Standard now reads: "Agencies shall avoid purchasing software for which support is not readily available."
Consolidate standard	040105	Implementing New / Upgraded Software	Consolidate standard.	Moved the following statements from 060111 – Installing Virus Scanning Software: "System configuration management regarding the installation of software shall include the following: o Maintenance of good backups of critical data and programs. o Periodic review of overall controls to determine weaknesses. o Limiting use of software to that which can be verified to be free of harmful code or other destructive aspects. o Complete information about the software shall be maintained, such as the vendor address and telephone number, the license number and version, and update information. o Configuration reports shall be maintained of all installed software, including the operating system. This information will be necessary if the software must be reinstalled later. o Software programs shall be reinstalled only from validated media. o Software shall be stored in a secure, tamper-proof location."

Goal	Section	Title	Comments/Update	Work Comments
Review/revise CVE requirements for patch management	040106	Technical Vulnerability Management	This requires that agencies track vulnerabilities by CVE. Since one to hundreds of CVE's could potentially be associated with one patch could this be left to the agency to track via an effective internal methodology and if needed be tracked back to the CVE?	**Response to customer.** Yes, as long the agency can track back to the CVE.
Review/update Vulnerability Management standard	040106	Technical Vulnerability Management	To avoid potential conflict from definition differences of "remediation" and "mitigation", recommend changing the word "remediated" to "mitigated" in this sentence. The first sentence in this standard seems to imply a requirement that mitigation of vulnerabilities be done through "updates and patches'.	Switched "mitigated" and "remediated for High-level risk vulnerabilities." Paragraph now reads, "'High-level risk' vulnerabilities must be mitigated as soon as possible. It is recommended that "High-level risk" vulnerabilities be mitigated within 7 days, and they must be remediated within 21 days."
Review/update Vulnerability Management standard	040106	Technical Vulnerability Management	Review/update requirements for vulnerability management. Include a category for "critical" vulnerabilities that must be patched ASAP.	Added the following bullet: "In the event of a zero-day vulnerability, a situation where an exploit is used before the developer of the software knows about the vulnerability, agencies shall mitigate the vulnerability immediately, If possible, and apply patches as soon as possible after the vendor provides them."
Consolidate standard	040201	Applying Patches to Software	Consolidate standard.	Moved the following statement from 060111 - Installing Virus Scanning Software: "System and application bug fixes or patches shall only be accepted from highly reliable sources, such as the software vendor."
Clarify requirement for two-factor authentication	050404	Working from Home or Other Off-Site Location (Teleworking)	Clarify statement on two-factor authentication in regards to required statute or industry standard.	Modified bullet to state the following: "Use of two-factor authentication products (such as one-time password tokens or biometric devices) to authenticate users, if applicable or if required by statute or industry standard (i.e. PCI DSS)"
Include mobile computing guidelines (i.e. ActiveSync)	050406	Using Mobile Communication Devices	Include guidelines from ITS Exchange policy on ActiveSync. Make generic vendor neutral guidelines.	Removed the following statement from the standard: "Personnel using mobile communication devices shall refrain from discussing topics considered confidential by the agency." Added "tablets" to the list of mobile communication devices. Added the following bullets: "Agencies that allow mobile communication devices (personal or business owned) to connect to enterprise state systems, such as e-Mail, shall require the following: o A minimum 4-digit numeric, user defined, personal identification number (PIN) that is changed every 90 days. o A time out of inactivity that is 10 minutes or less. o If technically possible, the ability to remotely erase the contents of the device, at the user's request, management request via a help desk service request, or by the user's own action. Agencies shall make end users aware that they are accepting the risk of personal data being lost. o Users shall report lost or stolen mobile communication devices to an agency's service desk or to agency management within 24 hours of confirmation."
Revise mobile computing guidelines	050406	Using Mobile Communication Devices	Revise guidelines.	Removed the following bullet from the guidelines: "If available, use a password to protect the device that follows statewide password policy standards." Added the following two bullets to the guidelines: "If possible, agencies should consider encrypting all mobile communication devices regardless of the confidentiality of the information stored on a device. o Users should utilize a remote wipe feature, if available, to remotely set the device to factory defaults if it is lost or stolen."
Review standard	050703	Insuring Hardware	Remove standard.	Removed standard.
Review standard	050704	Insuring Laptops/Portables for Use Domestically or Abroad	Remove standard.	Removed standard.
Review standard	050705	Clear Screen	Remove standard.	Removed standard. Already stated in 020103 - Securing Unattended Work Stations.
Review standard	050706	Logon and Logoff from your Computer	Remove standard.	Removed standard. Moved statement on locking workstations to standard 020103 - Securing Unattended Work Stations. Rest of standard is stated in 020102 and 020106.
Add PCI DSS requirements	060101	Defending Against Premeditated Cyber Crime Attacks	Add PCI DSS requirements.	Added the following PCI DSS requirements: "IDS/IPS signatures shall be up to date."

Goal	Section	Title	Comments/Update	Work Comments
Add PCI DSS requirements	060102	Minimizing the Impact of Cyber Attacks	Add PCI DSS requirements.	Added the following PCI DSS requirements: "Incident response plans shall incorporate information from intrusion detection/prevention systems (IDS/IPS), and other monitoring systems. Agencies shall develop a process to modify plans according to lessons learned and industry developments." Clarified requirements for BCP plans stating they "shall be tested at least annually per Standard 140104, Testing the Business Continuity Plan."
Add PCI DSS requirements	060109	Defending Against Virus Attacks	Consildate standard. Add PCI DSS requirements.	Moved the following standard from 060111 - Installing Virus Scanning Software: "Agencies shall install robust antivirus software on all LAN servers and workstations, including those used for remote access to the State network. In addition, system antivirus software, including virus signature files, shall be promptly updated as updates are released by the software vendor." Added the following PCI DSS requirements: "All virus scanning software shall be current, actively running on deployed workstations and servers, and capable of generating audit logs of virus events."
Consolidate standard	060111	Installing Virus Scanning Software	Consolidate standard.	Moved the following statement to 060109 - Defending Against Virus Attacks: "Agencies shall install robust antivirus software on all LAN servers and workstations, including those used for remote access to the State network. In addition, system antivirus software, including virus signature files, shall be promptly updated as updates are released by the software vendor." Moved the rest of the standard into 040105 - Implementing New / Upgraded Software and 040201 - Applying Patches to Software where applicable.
Review/revise virus mitigation strategies	060109 & 060110	Defending Against Virus Attacks	Suggest adding language to include adding any non-approved peripherals (such as USB drives, hard drives, or other hardware) or is this addressed in another standard? This requires that a virus outbreak of two or more computers be reported. Please clarify what is the requirement to report viruses on a network.	**Response to customer**: If the device is non-approved, it is not approved to be used and should not be addressed. Agencies shall report viruses when it becomes a significant event for the agency.
Clarify test environment requirements	080103	Controlling Software Code during Software Development	Clarify requirement for software changes to be tested.	Modified bullet in standard to say the following: "All changes must be tested in a test environment and must pass acceptance testing prior to moving changed code into a live or production environment."
Consolidate standard	080301	Controlling Test Environments	Consolidate standard.	Removed standard. It exists in 080103 - Controlling Software Code during Software Development.
Add PCI DSS requirements	080302	Using Live Data for Testing	Add PCI DSS requirements.	Added the following PCI DSS requirements: "Agencies shall permit the use of production data during the testing of new systems or systems changes only when no other alternative allows for the validation of the functions and when permitted by other regulations and standards. Confidential live data shall not be used for testing purposes"
Add PCI DSS requirements	080303	Testing Software before Transferring to a Live Environment	Add PCI DSS requirements.	Added the following PCI DSS requirements: "Test data and accounts shall be removed from an application or system prior to being deployed into a production environment. This does not apply to an application or system with a dedicated testing environment."
Define "Computing Facilities"	090104	Physical Access Control to Secure Areas	Please define computing facilities in the glossary to define the scope of this statement. Does this mean data center access or facilities that have any state computers (such as a house, conference center, etc).	Removed the following statement: "Agencies shall protect their computing facilities, locations and rooms from unauthorized access with appropriate physical access controls." Moved the following statement from standard 020107 - Securing Against Unauthorized Physical Access: "Agencies shall ensure areas housing information technology assets have appropriate physical access controls. Authorized individuals may include State employees, contractors and vendors. Agencies shall develop access policies for authorized individuals as well as visitors to these areas. An audit trail of access for all individuals to datacenters shall be maintained." Added the following PCI DSS requirements: "Agencies shall also restrict access to publicly accessible network jacks in datacenters by disabling unused network jacks, unless they are explicitly authorized. Physical access to wireless access points, networking equipment and cabling shall be restricted to only authorized personnel."

Goal	Section	Title	Comments/Update	Work Comments
Add PCI DSS requirements	090106	High Security Locations	Add PCI DSS requirements.	Added the following PCI DSS requirements: "Video cameras and/or access control mechanisms shall be used to monitor individual physical access to sensitive areas." Modified statement on camera, video recordser, etc. to say the following: "The use of personal cameras, video recorders and handheld devices (cell phones, PDAs, pocket PCs), shall be restricted from high security locations to protect the information being stored."
Review standard	090301	Electronic Eavesdropping	Modify auditing requirement for wireless LANs.	Included vulnerability assessment scans and operating system detection as a means to audit rogue access points. Also added recommendation to use wireless sniffers to scan. Standard now says the following: "Agencies using 802.11 wireless LANs must enable rogue access point detection in the management software of the WLAN, if available, and search their sites using wireless sniffers or vulnerability assessment scans and operating system detection at least quarterly to ensure that only authorized wireless access points are in place. Using wireless sniffers to scan and reviewing monthly is recommended. This type of audit is also recommended for sites not using wireless technologies to detect rogue access points and end-user-installed free-agent access points."
Review/revise WLAN standard	090301	Electronic Eavesdropping	Clarify scanning requirement for wireless airspace.	Clarified scope of the wireless monitoring requirement. Standard now states the following: "The management system shall monitor the airspace in and around agency facilities for unauthorized access points and ad hoc networks that are attached to the agency's network."
Clarify disaster recovery plan standard	090303	Disaster Recover Plan	Clarify standard.	Moved standard to chapter 14 and renumbered to 140107. Renamed title to be "Disaster Recovery and/or Restoration". Modified Purpose to be the following: To restore the operability of the systems supporting critical business processes and return to normal agency operations as soon as possible." Added the following statement and bullets: "Agencies shall conduct the following disaster recovery and/or restoration activities: o Define the agency's critical operating facilities and mission essential service(s) or function(s). o Define the resources (facilities, infrastructure, essential systems) that support each mission critical service or function. o Define explicit test objectives and success criteria to enable an adequate assessment of the Disaster Recovery and/or Restoration." Removed Related Information section.
Review standard	100109	Establishing Ownership of Intellectual Property Rights	Remove standard.	Removed standard.
Consolidate standard	100302	Keeping Passwords/PIN Numbers Confidential	Consolidate standard.	Moved standard to 020106 - Managing Passwords.
Consolidate standard	110101	Delivering Awareness Programs to Permanent Staff	Consolidate stnadard.	Moved the following statement from 110104 - Drafting Top Management Security Communications to Staff: "Senior management within the agency shall ensure that information security communications are given priority by staff and shall support information security education programs. All agencies shall provide new employees and contractors with mandatory information security training as part of job orientation."
Consolidate standard	110104	Drafting Top Management Security Communications to Staff	Consolidate standard.	Moved standard to 110101 - Delivering Awareness Programs to Permanent Staff.
Consolidate standard	120202	Complying with Information Security Standards and Policy	Consolidate standard.	Added the following statement from 120407 – Reviewing System Compliance Levels: "When penetration tests or vulnerability assessments are used, agencies must follow the requirements of G.S. §147-33.111(c)."
Add guidance for maintenance of evidence	120401	Recording Evidence of Information Security Incidents	What is the guidance from ITS on the maintenance of evidence for legal actions?	Some content already stated in 130101 - Reporting Information Security Incidents. Moved other content to standards 130202 - Collecting Evidence of an Information Security Breach. Removed standard 120401.

Goal	Section	Title	Comments/Update	Work Comments
Define "Regularly Reviewed"	120407	Reviewing System Compliance Levels	Please define regularly reviewed (not to exceed what time period?). According to the access control framework some systems are only reviewed on an ad-hoc basis. Please define qualified information technology personnel in the glossary of terms	Moved most content into 120202 - Complying with Information Security Standards and Policy. Removed standard 120407.
Review Incident Response standard.	130101	Reporting Information Security Incidents	The characteristics for incident severities 2 and 3 are identical in chart.	Renamed chapter title to be "Detecting and Responding to Information Technology Security Incidents." Modified chart in standard 130101 to match the ITS Incident Management Plan chart.
Consolidate standard	130105	Witnessing an Information Security Breach	Consolidate standard.	Added the following content from from 130106 – Being Alert for Fraudulent Activities: "Upon detection, suspected fraudulent activity shall be documented and reported to agency management in accordance with agency state and agency standards, policies and procedures for appropriate action as soon as possible."
Consolidate standard	130106	Being Alert for Fraudulent Activities	Consolidate standard.	Moved standard to 130105 - Witnessing an Information Security Breach.
Review/revise requirement for reporting lost/stolen devices	130108	Lost or Stolen Computer Equipment	The statute, N.C.G.S. §114-15.1, states that the person discovering the incident has three days to report the incident. 1) Does this change that legal requirement to less than three days after discovery? 2) If so, what is the time frame that an agency must be informed of the loss of an information asset?	**Response to customer.** 1) No. A policy manual can be more stringent than the legal requirement, but not less.
Clarify the word "agency"	130108	Lost or Stolen Computer Equipment	Clarify who the "agency" responsible for reporting an incident (i.e. the service provider/manager like ITS or the recepient/user of the equipment)	Clarified standard to say the following: "Recipients/end users must report loss or stolen state computer equipment (for example, workstations, laptops, mobile communication devices, etc.) immediately to their agency management. Their agency management shall then notify the responsible individual/organization of the security event."
Consolidate standard	130202	Collecting Evidence of an Information Security Breach	Consolidate standard.	Moved the following statement from 120401 - Recording Evidence of Information Security Incidents: "The collection process shall include a document trail, the chain of custody for items collected, and logs of all evidence-collecting activities to ensure the evidence is properly preserved for any legal actions that may ensue as a result of the incident."
Consolidate standard	130403	Monitoring Confidentiality and Reporting Breaches	Consolidate standard.	Renamed standard to be "Monitoring Confidentiality and Reporting Breaches." Moved the following statement from 130407 - Monitoring Confidentiality of Information Security Incidents: "Agencies shall monitor and control the release of confidential security information during the course of a security incident or investigation to ensure that only appropriate individuals have access to the information, such as law enforcement officials, legal counsel or human resources."
Consolidate standard	130405	Using Information Security Incident Reporting Form	Consolidate standard.	Removed standrd. Already mentioned in 130101 - Reporting Information Security Incidents.
Consolidate standard	130407	Monitoring Confidentiality of Information Security Incidents	Consolidate standard.	Moved standard to 130403 - Monitoring Confidentiality and Reporting Breaches.
Consolidate standard	130408	Risks in System Usage	Consolidate standard.	Moved standard to 030104 - Defending Network Information from Malicious Attack.
Consolidate standard	130409	Reviewing System Usage	Consolidate standard.	Moved standard to 030104 - Defending Network Information from Malicious Attack.
Correct section headers	140102	Assessing the BCP Risk	Clarify estimate of the maximum elapsed time and the maximum amount of information or data.	Added the following references: (See also Statewide Glossary for Recovery Time Objective) and (See also Statewide Glossary for Recovery Point Objective).
Move disaster recovery standard	140107	Disaster Recovery and/or Restoration Plan	Move standard 090303 - Disaster Recovery Plan to chapter 14.	Moved standard 090303 to 140107. See comments on 090303.

Goal	Section	Title	Comments/Update	Work Comments
Enhance standard to include Risk Type Classifications	150101	Implementing a Risk Management Program	Review and update as necessary risk classifications to potentially include federal guidelines.	Included the following information from the Risk Management Guide: "In general, “risk” is defined as the potential exposure of an activity to damage. Some types of risk are as follows: • Business Risk – The cost and/or lost revenue associated with an interruption to normal business operations. • Organizational Risk – The direct or indirect loss resulting from one or more of the following: o Inadequate or failed internal processes o People o Systems o External events • Information Technology Risk- The loss of an automated system, network or other critical information technology resource that would adversely affect business processes."
Review risk management standard	150101	Implementing a Risk Management Program	Chapter 15 should provide some precise uniform metrics for all of state government. Chapter 15 should also provide some templates and examples of how to tabulate risk management, some examples could be found at http://cisr.mit.edu.	Added the following statement: "For more information on implementing a risk management program, including the Risk Management Guide and the Risk Assessment Questionnaire, please refer to the Risk Management Services page found on the Enterprise Security and Risk Management Office (ESRMO) web site: http://www.esrmo.scio.nc.gov/riskManagement/default.aspx"
Review standard	150101	Implementing a Risk Management Program	The reference here to "risks associated with the agency's business" broadens the scope to those risk matters that might be beyond the control of IT. The management of business risk should be the responsibility of a more appropriate business representative.	Added a reference to the Risk Management Services page on the ESRMO web site.
Review standard	150101	Implementing a Risk Management Program	Suggest rewording "information technology systems and resources" to include information assets since it is already defined.	**Response to customer:** Adding "information assets" to that statement in the standard would not be a good fit. Information assets includes the data itself.
Add/Modify glossary term	Glossary		Modify definition of "Application Domain"	Modified definition
Add/Modify glossary term	Glossary		Add definiton for "Credentials"	Added definition.
Add/Modify glossary term	Glossary		Modify definition of "Infrasructure"	Modified definition
Add/Modify glossary term	Glossary		Modify definition of "Inter-Agency WAN" to be public	Modified definition
Add/Modify glossary term	Glossary		Add definition for "Intrusion Prevention System"	Added definition.
Add/Modify glossary term	Glossary		Add definiton for "Mobile Code"	Added definition.
Add/Modify glossary term	Glossary		Add definition for "Private Network"	Added definition.
Add/Modify glossary term	Glossary		Add definition for "Public Network"	Added definition.
Add/Modify glossary term	Glossary		Modify definition for "Recovery Time Actual (RTA)"	Modified definition.